OSI model

From Wikipedia, the free encyclopedia

OSI Model
7 Application Layer
6 Presentation Layer
5 Session Layer
4 Transport Layer
3 Network Layer
2 Data Link Layer ■ LLC sublayer ■ MAC sublayer
1 Physical Layer

The **Open Systems Interconnection Basic Reference Model** (OSI Reference Model or **OSI Model**) is an abstract description for layered communications and computer network protocol design. It was developed as part of the Open Systems Interconnection (OSI) initiative[1]. In its most basic form, it divides network architecture into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data-Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model**.

A layer is a collection of conceptually similar functions that provide services to the layer above it and receives service from the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of the path.

Even though it has been largely superseded by newer IETF, IEEE, and indeed OSI protocol developments (subsequent to the publication of the original architectural standards), the basic OSI model is considered an excellent place to begin the study of network architecture. Not understanding that the pure seven-layer model is more historic than current, many beginners make the mistake of trying to fit every protocol under study into one of the seven basic layers. Especially the attempts of cross-layer optimization break the boundaries of the original layer scheme. Describing the actual layer concept with implemented systems is not always easy to do as most of the protocols in use on the Internet were designed as part of the TCP/IP model, and may not fit cleanly into the OSI Model.

Contents

History

In 1977, work on a layered model of network architecture was started, and the International Organization for Standardization (ISO) began to develop its OSI framework architecture. The ISO is a worldwide federation of national standards bodies from some 130 countries, one from each country. OSI has two major components: an abstract model of networking (the Basic Reference Model, or seven-layer model) and a set of specific protocols. The standard documents that describe the OSI model can be freely downloaded from the ITU-T as the **X.200**-series of recommendations [2]. A number of the protocol specifications are also available as part of the ITU-T X series. The equivalent ISO and ISO/IEC standards for the OSI model are available from the ISO, but only some of the ISO/IEC standards are available as cost-free downloads.[3]

Some aspects of OSI design evolved from experiences with the CYCLADES network, which also influenced Internet design. The new design was documented in ISO 7498 and its various addenda. In this model, a networking system is divided into layers. Within each layer, one or more entities implement its functionality. Each entity interacts directly only with the layer immediately beneath it, and provides facilities for use by the layer above it.

Protocols enable an entity in one host to interact with a corresponding entity at the same layer in another host. Service definitions abstractly describe the functionality provided to an (N)-layer by an (N-1) layer, where N is one of the seven layers of protocols operating in the local host.

Description of OSI layers

Remembering The OSI Layers

OSI Model

Various mnemonics have been created over the years to help remember the order, such as:

- **A**ll **P**eople **S**eem **T**o **N**eed **D**ata **P**rocessing
- **P**lease **D**o **N**ot **T**ake **S**ales-**P**eople's **A**dvice
- **P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way

	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Interhost communication
	Segment	4. Transport	End-to-end connections and reliability (TCP)
Media layers	Packet/Datagram	3. Network	Path determination and logical addressing (IP)
	Frame	2. Data Link	Physical addressing (MAC & LLC)
	Bit	1. Physical	Media, signal and binary transmission

Layer 7: Application Layer

This Application Layer interface directly performs application services for the application processes; it also issues requests to the presentation layer. Note carefully that this layer provides services to user-defined application processes, and not to the end user. For example, it defines a file transfer protocol, but the end user must go through an application process to invoke file transfer. The OSI model does not include human interfaces. The common application services sublayer provides functional elements including the Remote Operations Service Element (comparable to Internet Remote Procedure Call), Association Control, and Transaction Processing (according to the ACID requirements).

Above the common application service sublayer are functions meaningful to user application programs, such as messaging (X.400), directory (X.500), file transfer (FTAM), virtual terminal (VTAM), and batch job manipulation (JTAM). These contrast with user applications that use the *services* of the application layer, but are not part of the application layer itself.

1. File Transfer applications using FTAM (OSI protocol) or FTP (TCP/IP Protocol)
2. Mail Transfer clients using X.400 (OSI protocol) or SMTP/POP3/IMAP (TCP/IP protocols)
3. Web browsers using HTTP (TCP/IP protocol); no true OSI protocol for web applications

Layer 6: Presentation Layer

The Presentation Layer establishes a context between application layer entities, in which the higher-layer entities can use different syntax and semantics, as long as the Presentation Service understands both and the mapping between them. The presentation service data units are then encapsulated into Session Protocol Data Units, and moved down the stack.

The original presentation structure used the Basic Encoding Rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serializing objects and other data structures into and out of XML. ASN.1 has a set of cryptographic encoding rules that allows end-to-end encryption between application entities.

Layer 5: Session Layer

The Session Layer controls the dialogues/connections (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for "graceful close" of sessions, which is a property of TCP, and also for session checkpointing and recovery, which is not usually used in the Internet protocol suite. Session layers are commonly used in application environments that make use of remote procedure calls (RPCs).

Layer 4: Transport Layer

The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the transport layer can keep track of the segments and retransmit those that fail.

Although not developed under the OSI Reference Model and not strictly conforming to the OSI definition of the Transport Layer, the best known examples of a Layer 4 protocol are the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

Of the actual OSI protocols, there are five classes of transport protocols ranging from class 0 (which is also known as **TP0** and provides the least error recovery) to class 4 (which is also known as **TP4** and is designed for less reliable networks, similar to the Internet). Class 0 is closest to UDP. Class 4 is closest to TCP, although TCP contains functions, such as the graceful close, which OSI assigns to the Session Layer. Detailed characteristics of TP0-4 classes are shown in the following table:[4]

Feature Name	TP0	TP1	TP2	TP3	TP4
Connection oriented	-	-	-	Yes	Yes
Connectionless	-	-	-	No	Yes
Segmentation/Fragmentation	Yes	Yes	Yes	Yes	Yes
Reassembly	Yes	Yes	Yes	Yes	Yes

Error Recovery	No	Yes	No	No	Yes
Reinitiate connection (if an excessive number of PDUs are unacknowledged)	No	Yes	No	Yes	Yes
multiplexing and demultiplexing over a single virtual circuit	No	No	Yes	Yes	Yes
Reliable Transport Service	No	Yes	Yes	Yes	Yes

Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent. Do remember, however, that a post office manages the outer envelope of mail. Higher layers may have the equivalent of double envelopes, such as cryptographic presentation services that can be read by the addressee only. Roughly speaking, *tunneling protocols* operate at the transport layer, such as carrying non-IP protocols such as IBM's SNA or Novell's IPX over an IP network, or end-to-end encryption with IPsec. While Generic Routing Encapsulation (GRE) might seem to be a network layer protocol, if the encapsulation of the payload takes place only at endpoint, GRE becomes closer to a transport protocol that uses IP headers but contains complete frames or packets to deliver to an endpoint. L2TP carries PPP frames inside transport packet.

Layer 3: Network Layer

The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer—sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme – values are chosen by the network engineer. The addressing scheme is hierarchical.

The best-known example of a Layer 3 protocol is the Internet Protocol (IP). It manages the connectionless transfer of data one hop at a time, from end system to ingress router, router to router, and from egress router to destination end system. It is not responsible for reliable delivery to a next hop, but only for the detection of errored packets so they may be discarded. When the medium of the next hop cannot accept a packet in its current length, IP is responsible for **fragmenting** into sufficiently small packets that the medium can accept it.

A number of layer management protocols, a function defined in the Management Annex, ISO 7498/4, belong to the Network Layer. These include routing protocols, multicast group management, Network Layer information and error, and Network Layer address assignment. It is the function of the payload that makes these belong to the network layer, not the protocol that carries them.

Layer 2: Data Link Layer

The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. Originally, this layer was intended for point-to-point and point-to-multipoint media, characteristic of wide area media in the telephone system. Local area network architecture, which included broadcast-capable multiaccess media, was developed independently of the ISO work, in IEEE Project 802. IEEE work assumed sublayering and management functions not required for WAN use. In modern practice, only error detection, not flow control using sliding window, is present in modern data link protocols such as Point-to-Point Protocol (PPP), and, on local area networks, the IEEE 802.2 LLC layer is not used for most protocols on Ethernet, and, on other local area networks, its flow control and acknowledgment mechanisms are rarely used. Sliding window flow control and acknowledgment is used at the transport layers by protocols such as TCP, but is still used in niches where X.25 offers performance advantages.

Both WAN and LAN services arrange bits, from the physical layer, into logical sequences called frames. Not all Physical Layer bits necessarily go into frames, as some of these bits are purely intended for Physical Layer functions. For example, every fifth bit of the FDDI bit stream is not used by the Data Link Layer.

WAN Protocol architecture

Connection-oriented WAN data link protocols, in addition to framing, detect and may correct errors. They also are capable of controlling the rate of transmission. A WAN Data Link Layer might implement a sliding window flow control and acknowledgment mechanism to provide reliable delivery of frames; that is the case for SDLC and HDLC, and derivatives of HDLC such as LAPB and LAPD.

IEEE 802 LAN architecture

Practical, connectionless LANs began with the pre-IEEE Ethernet specification, which is the ancestor of IEEE 802.3. This layer manages the interaction of devices with a shared medium, which is the function of a Media Access Control sublayer. Above this MAC sublayer is the media-independent IEEE 802.2 Logical Link Control (LLC) sublayer, which deals with addressing and multiplexing on multiaccess media.

While IEEE 802.3 is the dominant wired LAN protocol and IEEE 802.11 the wireless LAN protocol, obsolescent MAC layers include Token Ring and FDDI. The MAC sublayer detects but does not correct errors.

Layer 1: Physical Layer

The Physical Layer defines all the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium. This includes the layout of pins, voltages, cable specifications, Hubs, repeaters, network adapters, Host Bus Adapters

(HBAs used in Storage Area Networks) and more.

To understand the function of the Physical Layer in contrast to the functions of the Data Link Layer, think of the Physical Layer as concerned primarily with the interaction of a single device with a medium, where the Data Link Layer is concerned more with the interactions of multiple devices (i.e., at least two) with a shared medium. The Physical Layer will tell one device how to transmit to the medium, and another device how to receive from it (in most cases it does not tell the device how to connect to the medium). Obsolescent Physical Layer standards such as RS-232 do use physical wires to control access to the medium.

The major functions and services performed by the Physical Layer are:

- Establishment and termination of a connection to a communications medium.
- Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- Modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

Parallel SCSI buses operate in this layer, although it must be remembered that the logical SCSI protocol is a Transport Layer protocol that runs over this bus. Various Physical Layer Ethernet standards are also in this layer; Ethernet incorporates both this layer and the Data Link Layer. The same applies to other local-area networks, such as Token ring, FDDI, and IEEE 802.11, as well as personal area networks such as Bluetooth and IEEE 802.15.4.

Interfaces

Neither the OSI Reference Model nor OSI protocols specify any programming interfaces, other than as deliberately abstract service specifications. Protocol specifications precisely define the interfaces between different computers, but the software interfaces inside computers are implementation-specific.

For example, Microsoft Windows' Winsock, and Unix's Berkeley sockets and System V Transport Layer Interface, are interfaces between applications (layers 5 and above) and the transport (layer 4). NDIS and ODI are interfaces between the media (layer 2) and the network protocol (layer 3).

Interface standards, except for the Physical Layer to media, are approximate implementations of OSI Service Specifications.

Examples

Layer		Misc. examples	TCP/IP suite	SS7[5]	AppleTalk suite	OSI suite	IPX suite	SNA	UMTS
#	Name								
7	Application	HL7, Modbus	NNTP, SIP, SSI, DNS, FTP, Gopher, HTTP, NFS, NTP, DHCP, SMPP, SMTP, SNMP, Telnet	INAP, MAP, TCAP, ISUP, TUP	AFP, ZIP, RTMP, NBP	FTAM, X.400, X.500, DAP, ROSE, RTSE, ACSE	RIP, SAP	APPC	
6	Presentation	TDI, ASCII, EBCDIC, MIDI, MPEG	MIME, XDR, SSL, TLS (Not a separate layer)		AFP	ISO/IEC 8823, X.226, ISO/IEC 9576-1, X.236			
5	Session	Named Pipes, NetBIOS, SAP, Half Duplex,Full Duplex,Simplex,SDP	Sockets. Session establishment in TCP. SIP. (Not a separate layer with standardized API.)		ASP, ADSP, PAP	ISO/IEC 8327, X.225, ISO/IEC 9548-1, X.235	NWLink	DLC?	
4	Transport	NBF, nanoTCP, nanoUDP	TCP, UDP,PPTP, L2TP, SCTP, RTP		DDP	ISO/IEC 8073, TP0, TP1, TP2, TP3, TP4 (X.224), ISO/IEC 8602,	SPX		

						X.234			
3	Network	NBF, Q.931	IP, IPsec, ARP, ICMP, RIP, OSPF, BGP, IGMP, IS-IS	SCCP, MTP	ATP (TokenTalk or EtherTalk)	ISO/IEC 8208, X.25 (PLP), ISO/IEC 8878, X.223, ISO/IEC 8473-1, CLNP X.233.	IPX		RRC (Radio Resource Control) Packet Data Convergence Protocol (PDCP) and BMC (Broadcast/Multicast Control)
2	Data Link	802.3 (Ethernet), 802.11a/b/g/n MAC/LLC, 802.1Q (VLAN), ATM, HDP, FDDI, Fibre Channel, Frame Relay, HDLC, ISL, PPP, Q.921, Token Ring, CDP	PPP, SLIP	MTP, Q.710	LocalTalk,AppleTalk Remote Access, PPP	ISO/IEC 7666, X.25 (LAPB), Token Bus, X.222, ISO/IEC 8802-2 LLC Type 1 and 2	IEEE 802.3 framing, Ethernet II framing	SDLC	LLC (Logical Link Control), MAC (Media Access Control)
1	Physical	RS-232, V.35, V.34, I.430, I.431, T1, E1, 10BASE-T, 100BASE-TX, POTS, SONET, SDH,DSL, 802.11a/b/g/n PHY		MTP, Q.710	RS-232, RS-422, STP, PhoneNet	X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703)		Twinax	UMTS L1 (UMTS Physical Layer)

Humor

The seven layer model is sometimes humorously extended to refer to non-technical issues or problems. A common joke is the 10 layer model, with layers 8, 9, and 10 being the "user", "financial", and "political" layers, or the "money", "politics", and "religion" layers. Similarly, network technicians will sometimes refer to "layer-eight problems", meaning problems with an end user and not with the network.

Comparison with TCP/IP

In the TCP/IP model of the Internet, protocols are deliberately not as rigidly designed into strict layers as the OSI model.[6] RFC 3439 contains a section entitled "Layering considered harmful." However, TCP/IP does recognize four broad layers of functionality which are derived from the operating scope of their contained protocols, namely the scope of the software application, the end-to-end tranport connection, the internetworking range, and lastly the scope of the direct links to other nodes on the local network.

Even though the concept is different than in OSI, these layers are nevertheless often compared with the OSI layering scheme in the following way: The Internet Application Layer includes the OSI Application Layer, Presentation Layer, and most of the Session Layer. Its end-to-end Transport Layer includes the graceful close function of the OSI Session Layer as well as the OSI Transport Layer. The internetworking layer (Internet Layer) is a subset of the OSI Network Layer, while the Link Layer includes the OSI Data Link and Physical Layers, as well as parts of OSI's Network Layer. These comparisons are based on the original seven-layer protocol model as defined in ISO 7498, rather than refinements in such things as the internal organization of the Network Layer document.

The presumably strict consumer/producer layering of OSI as it is usually described does not present contradictions in TCP/IP, as it is permissible that protocol usage does not follow the hierarchy implied in a layered model. Such examples exist in some routing protocols (e.g., OSPF), or in the description of tunneling protocols, which provide a Link Layer for an application, although the tunnel host protocol may well be a Transport or even an Application Layer protocol in its own right.

The TCP/IP design generally favors decisions based on simplicity, efficiency and easy of implementation.

References

1. ^ reference needed
2. ^ ITU-T X-Series Recommendations.
3. ^ Publicly Available Standards
4. ^ "ITU-T Recommendation X.224 (11/1993) [ISO/IEC 8073]". Retrieved on 2008-06-18.
5. ^ ITU-T Recommendation Q.1400 (03/1993), *Architecture framework for the development of signalling and OA&M protocols using OSI concepts*, pp 4, 7.
6. ^ RFC 3439

External links

- (license agreement for downloading) and ISO/IEC standard 7498-1:1994 (ZIP format)
- ITU-T X.200 (the same contents as from ISO)
- OSI Reference Model — The ISO Model of Architecture for Open Systems Interconnection PDF (776 KB), Hubert Zimmermann, IEEE Transactions on Communications, vol. 28, no. 4, April 1980, pp. 425 - 432.
- Internetworking Basics

Retrieved from "http://en.wikipedia.org/wiki/OSI_model"
Categories: CISSP | Network architecture | ISO standards | ITU-T recommendations | OSI protocols | Reference models
Hidden categories: Articles needing additional references from February 2008 | All articles with unsourced statements | Articles with unsourced statements since June 2008